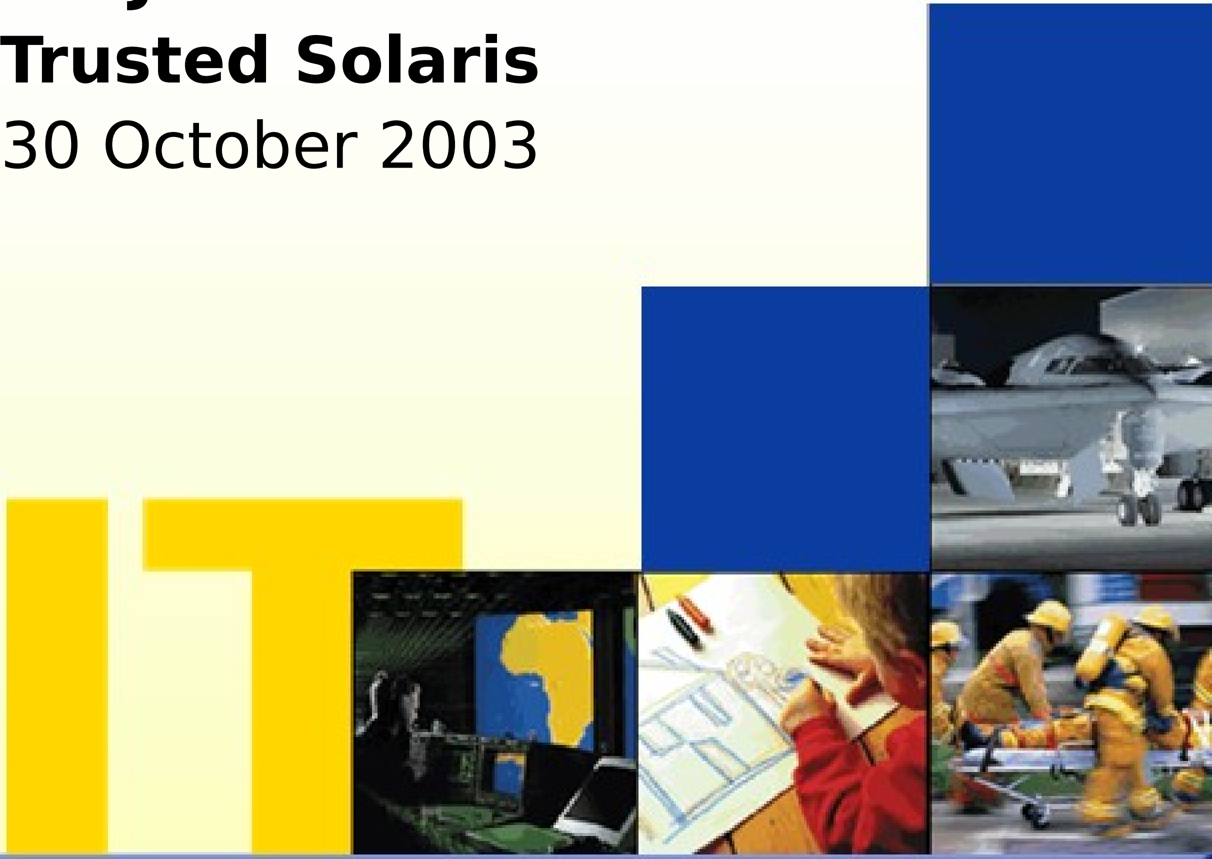
JEDI 2.0
Trusted Solaris

30 October 2003



JEDI Trusted Solaris (TSol)

- **The goal of the JEDI TSol design is to be identical to the JEDI design for Solaris 9 with some deviations based on requirements**
  - Identical RBAC, SMC design
    - This will not be a “re-hash” of the JEDI Solaris 9 design
      - This is more of a requirements validation to discuss deviations from the Solaris 9 JEDI 2.0 design

JEDI Trusted Solaris (TSol)

- **Deviations from the Solaris 9 design will be limited to:**
  - Issues with naming services “supported
  - Support for Multi Level Directory (MLD) and Single Level Directory (SLD) structures for select JEDI utilities
  - JEDI Audit Collection, Reduction, Review, and Archive utilities
  - JEDI Host Maintenance support for TSol unique tables
  - Removal of duplicative JEDI utilities
  - Inclusion and configuration of Trusted Solaris 8 IP Filters
  - Cross security domain administration
- **Issues**

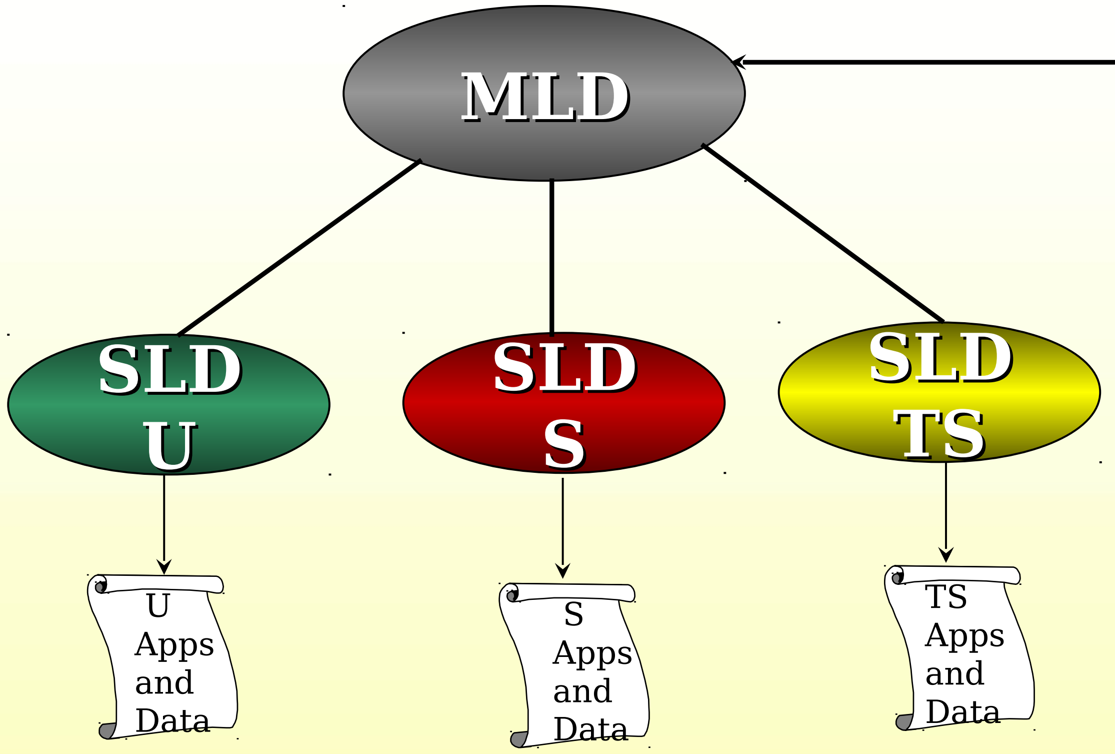
JEDI TSol Naming Services Issues

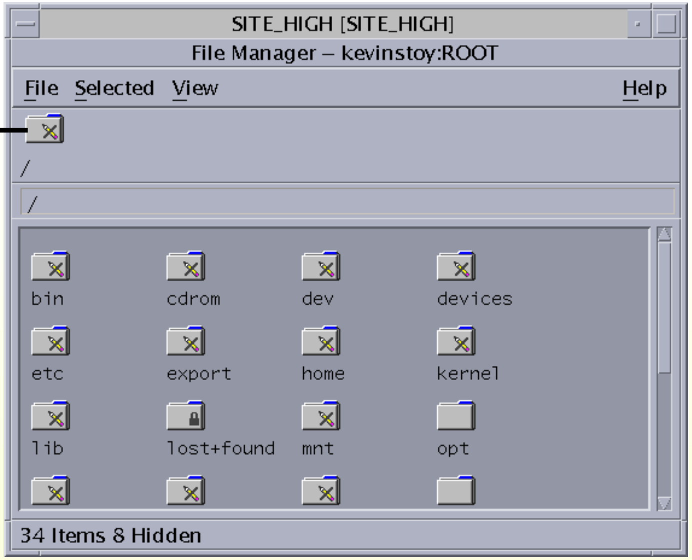
- **Naming Services “Supported” with JEDI for TSol will be limited to Local /etc files, DNS, and NIS+**
- **NIS and LDAP will not be “supported”**
  - TSol will support these naming services but has not been through a Common Criteria Evaluation in these configurations
    - *Can we get these naming services through a PL4 certification without adversely affecting schedule?
      - Common Criteria Evaluation Assurance Level (EAL) 4 certification
        - Measured against the Label Security Protection Profile, Controlled Action Protection Profile, and the Role Based Access Control Protection Profile
      - DICAST approval to proceed
      - PL4 certification

*Further discussion with security personnel is required

JEDI Utilities to support MLD/SLD Structures

- **TSol Multi and Single Level Directory Structures (MLD/SLD)**





SITE_HIGH [SITE_HIGH]

File Manager – kevinstoy:ROOT

34 Items 8 Hidden

JEDI Utilities to support MLD/SLD Structures

- **Certain JEDI Utility functions will need to support TSol MLD/SLD structures**
  - Session Maintenance function
    - Session Maintenance and bld_mwmrc will be able to build the root menu and place it into a MLD home directory structure
  - Add User function
    - Will be MLD aware to create SLD home directories
  - DNS setup will be able to support creation of SLD resolve.conf files
    - Different security domains/networks will require different DNS configurations/servers/domain names

JEDI Audit Collection, Reduction, Review, and Archive utilities

- **Centralized Log and Audit Support Subsystem (CLASS)**
  - PACOM TWS configuration was written up with a CAT 2 security finding because it was running CLASS to process audit data
    - In TSol, audit files and the audit process are owned by Admin_High (highest security level on the system)
      - Accreditor did not want to see a process constantly running at Admin_High (class_client)
    - JWICS is only accredited to pass SI/TK traffic
      - More than just SI/TK being processed on the network
        - CLASS does not encrypt audit data sent from client to server
- **JEDI client process will not be constantly running and audit data will be transferred encrypted**

JEDI Host Maintenance Support for TSol Unique Tables

- **TSol comes with additional tables for managing hosts and network interfaces**
  - Trusted network interface database (tnidb), Trusted network remote hosts database (tnrhdb), Trusted network remote host template (tnrhtp), IP Filters configuration
  - The current SMC “Add Computer” function in TSol does not add the computer in all relevant tables or have fields for IP Filtering when adding hosts to the naming service table
    - At a minimum JEDI for TSol will support the Trusted network remote hosts database (tnrhdb) as well as the standard host table (/etc/hosts, hosts.org_dir)

Remove Duplicative JEDI utilities

- **Certain functions of JEDI are duplicative of what already comes with the TSol Operating System. These will be removed from the JEDI TSol baseline**
  - Allocate/Deallocate GUI is already supplied as a TSol authorized right requiring assignment by a trusted user
  - The JEDI security banner is unnecessary as all TSol windows are labeled
  - Shell is already protected by the TSol OS as an authorized right requiring assignment by a trusted user
  - Print Utility is not needed because all printed output on TSol is labeled with the security classification of the application the spooled the print job

IP Filters

- **JEDI will include the TSol 8 IP Filters**
  - SunScreen V3.2
    - Rules-based, dynamic packet-filtering engine for network-access control
    - Versatile firewall used for access control, authentication,and network data encryption
    - Administration is provided through a graphical user interface (GUI) accessed via a web browser or a command line interface
    - Product is bundled with Solaris 9 and Trusted Solaris 8 but customers must have a current Sun Enterprise Services support agreement for Solaris 9 Operating System or Trusted Solaris 8 Operating Environment to use
      - Otherwise the cost is $14,995

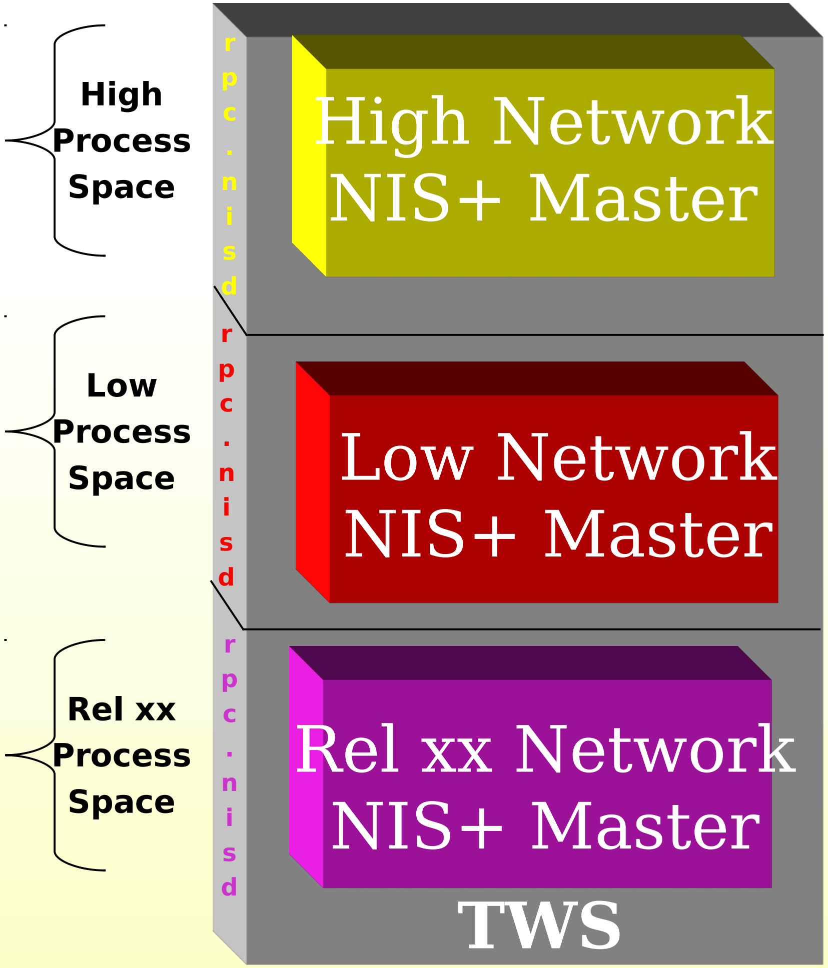
IP Filters

- **Suggestion for the TSol design is that we provide policy templates based on PACOM IP Filter rules**
- ***Do we include the SunScreen SKIP plug-in?**
  - – SKIP provides an IP-layer encryption and authentication software module that creates secure virtual private networks
    - Cost is $149 per workstation

***"Sun has focused future efforts beyond SunScreen 3.2 towards more fully integrating stateful Packet filtering into the Solaris OS rather than producing separate layered firewall products"**

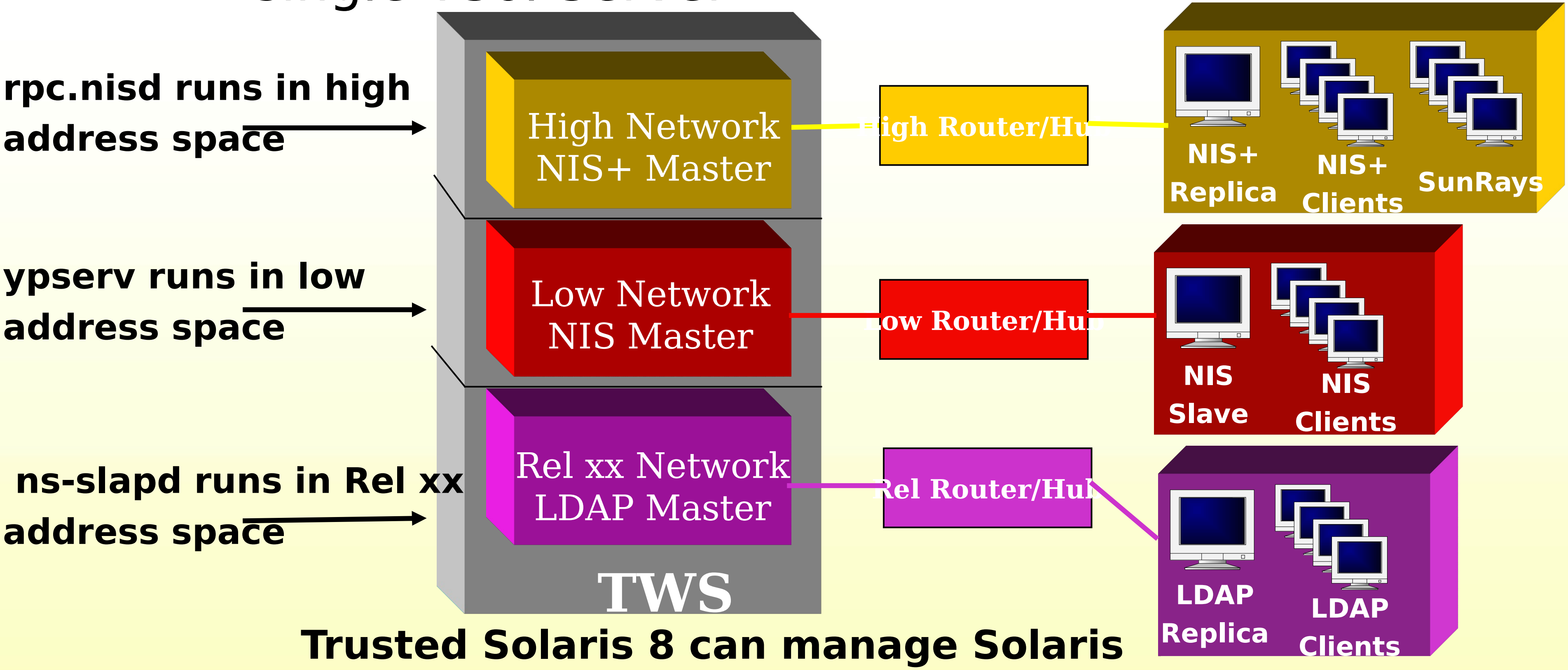
Cross Security Domain Administration

- **With Trusted Solaris 8 each process runs in it's own classification labeled process space**
  - Theoretically, you could run multiple instantiations of a naming service at differing classification levels
    - i.e., rpc.nisd at multiple classification process levels



Cross Security Domain Administration

- **Are there requirements for cross domain administration?**
  - Administer NIS, NIS+, LDAP domains from a single TSol Server



Trusted Solaris 8 can manage Solaris Clients as long as the Trusted machine is the Master

Issues

- **Solaris 9 uses the SMC v2.1, Trusted Solaris 8 uses SMC v2.0**
- **Solaris 9 SMC is built on JAVA V1.4, Trusted Solaris 8 SMC is built on JAVA V1.2.2**
  - Particular attention will go into building JEDI 2.0 to ensure it’s backward compatibility with JEDI for TSol
- **Additional Requirements or questions?**
  - Dynamic background menus based on Desktop Security Label?
  - Support for remote management of headless TSol Servers?